SECS 1030

labo Phishing email

Noté sur 13 points – 10% de la note finale à rendre pour

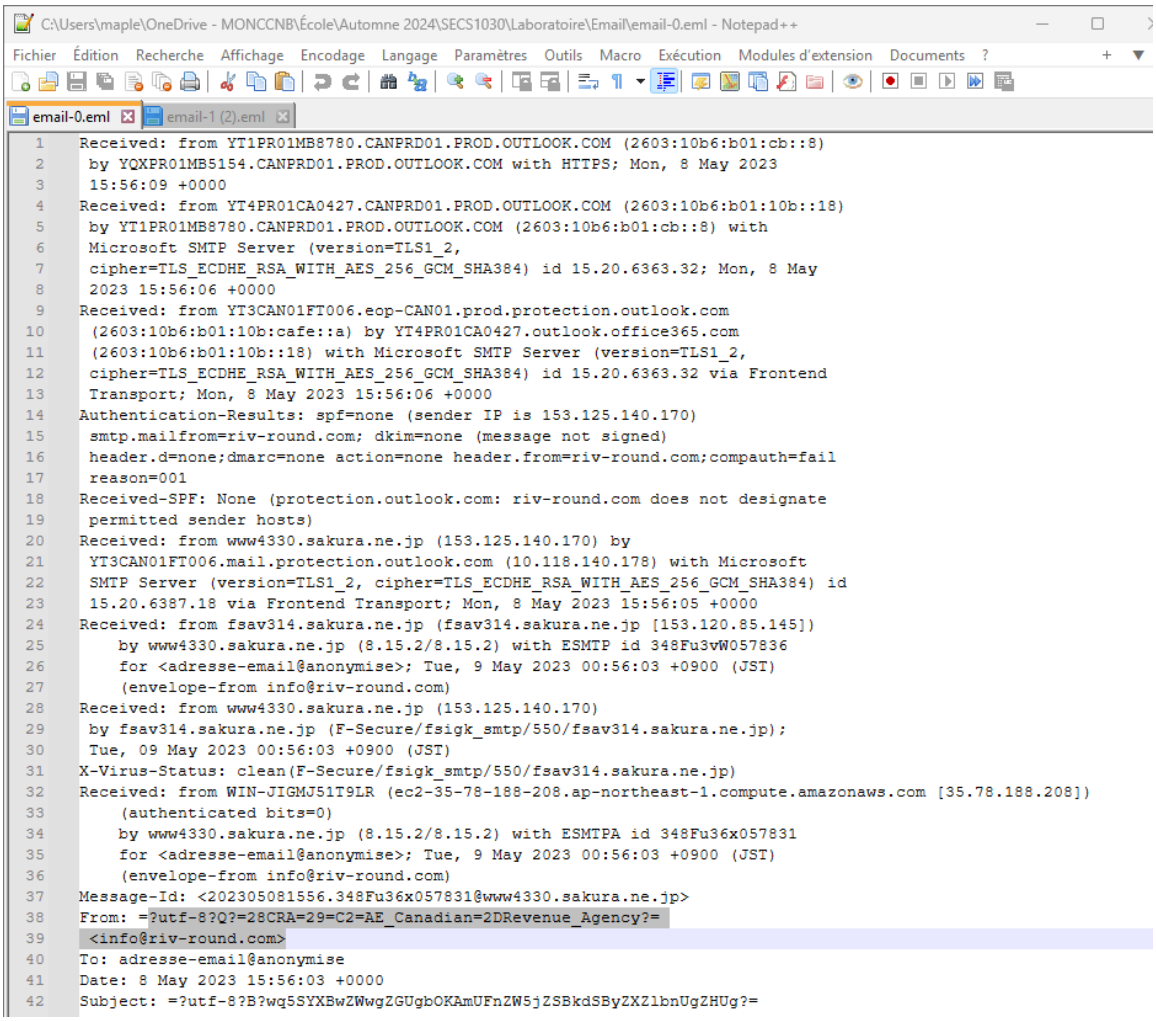
jeudi 17 octobre 2024 dans le casier de dépôt

Objectif du laboratoire : analyser 3 sources de courriels pour détecter une attaque de Phishing

Outil : un éditeur de fichier txt (notepad, notepad++, …) ou un éditeur de mail header. Les courriels sont sur Ardoise, Labos, labos email phishing

Exercice 0 : email-0.eml (3 points)

1. Quelle est la valeur dans le champ « from : » ? (text+addresse email)



2. Dans le champ « from : » , le texte (partie gauche) est-il cohérent avec l'adresse (partie entre <>) ?
   Non il n'est pas cohérent

3. Faites une recherche whois sur le domaine de l'adresse de « from : ». Quel est le nom et pays du registrant ? Pouvez-vous en déduire si ce courriel est un spoofing email ? Si oui pourquoi ?

   SHOTA OMARU, Japon, Je dirais que oui puisque le email est envoyer avec riv-round.com mais le message dit que ça vient de l'agence de revenu du Canada. C'est très suspect.

Exercice 1 : email1.eml (6 points)

1. Quel est le champ « from : » ? (text+adress)
   ?UTF-8?B?Y2hyb25vLXBvc3RlLWV4cHJlc3M=?=" <GNxHHUed@gktlbxlnC.us>
   Dans le champ « from : » , le texte est-il cohérent avec l'adresse ?

   Non

2. Est-ce que l'adresse email du champ « return_path » est la même que le champs « from: » ?

   non

3. Quel est le résultat de SPF ? Qu'est ce que ce résultat signifie ?
   Pass , l'adresse de retour est autorisé à envoyé

4. L'email contient-il un ou des liens ? Sur quel site pourriez-vous vérifiez ce lien ?

   Oui, virus total, url extractor, phishtool

5. Selon vous ce mail est-il un spam email ou un phishing email ?

   phishing

Exercice 2 : Questions (4 points)

1. Quelle commande permet d'afficher les adresses IP des serveurs emails autorisés pour le domaine outlook.com ? Montrez une capture écran du résultat :

   Dig TXT outlook.com +short

2. SPF : pour le domaine outlook.com, que signifie le mechasnism « ~all » à la fin de la ressource TXT « spf » du DNS record ?

   Il accpete les messages provenant d'expediteur qui ne figure pas dans l'enregistrement SPF, il les marque comme suspect.

3. Quelle commande permet d'afficher la clé publique du domaine gmail.com avec le selector 20230601 ?

   dig TXT 20230601._domainkey.gmail.com

4. Quelle commande permet d’afficher la règle DMARC pour le domaine outlook.com ?

   Dig TXT _dmarc.outlook.com